

CLAIMS

We claim:

1 1. Method for nesting connections between a plurality of
2 nodes in a communication network, comprising the steps
3 of:

4 receiving at a first node on an outer connection a
5 request from a second node to establish a coincident
6 endpoint for nesting an inner connection within said
7 outer connection;

8 negotiating over said outer connection parameters
9 defining said inner connection; and thereafter

10 responsive to communication occurring on said inner
11 connection, at said first node linking to said outer
12 connection for selectively receiving or sending said
13 communication double nested on said outer connection.

1 2. The method of claim 1, said inner connection being a
2 secure connection.

1 3. The method of claim 2, said inner connection being an
2 IPsec connection.

1 4. The method of claim 3, further comprising the step of
2 using Layer 2 Tunnel Protocol (L2TP) to tunnel packets
3 across said communication network.

1 5. Method for operating an enterprise gateway, comprising
2 the steps of:

3 receiving at said gateway from a remote client a
4 request to establish an outer connection;

5 receiving at said gateway over said outer connection a
6 request to establish, and thereupon negotiating
7 parameters establishing, a secure inner connection;

8 responsive to outbound or inbound traffic on said inner
9 connection, establishing links to said outer connection
10 for communicating said traffic double nested on said
11 outer connection.

1 6. The method of claim 5, further comprising the step of:

2 establishing a local coincident endpoint of said inner
3 and outer connections at said gateway.

1 7. The method of claim 5, further comprising the step of:

2 tunneling packets across said communication network
3 using Layer 2 Tunnel Protocol (L2TP).

1 8. A method for operating a first one of a plurality of
2 nodes in a communications network, comprising the steps
3 of:

4 establishing at said first node a coincident endpoint
5 for an outer connection and an inner connection with at
6 least one second node in said network;

7 responsive to starting communication of traffic over
8 said connections, establishing a link from said inner
9 connection to said outer connection; and

10 responsive to said links, selectively encapsulating
11 said traffic to said outer connection for transfer to

12 said second node or decapsulating said traffic from
13 said outer connection for receipt at said first node.

1 9. The method of claim 8, said inner connection being a
2 secure connection.

1 10. The method of claim 8, further comprising the step of:

2 tunneling packets across said communication network
3 using Layer 2 Tunnel Protocol (L2TP).

1 11. Method for for nesting connections between a plurality
2 of nodes in a communication network, said nodes
3 including a client, and internet service provider
4 (ISP), an enterprise gateway, and an internal network,
5 comprising the steps of:

6 operating said client node to call said ISP node;

7 operating said ISP node to start an outer connection
8 with respect to said gateway node and to return an IP
9 address to said client node;

10 operating said client node to send to said gateway node

11 over said outer connection a request to establish a
12 secure nested inner connection;

13 operating said client node and said gateway node to
14 negotiate over said outer connection parameters
15 defining said secure nested inner connection, and
16 saving said parameters at said gateway node; and
17 thereafter

18 operating said client node to start said inner
19 connection; and

20 operating said gateway node to recognize the start of
21 said inner connection and to link said inner connection
22 to said outer connection.

1 12. The method of claim 11, further comprising the steps
2 of:

3 sending outbound traffic in said inner connection
4 double nested in said outer connection.

1 13. The method of claim 12, further comprising the steps
2 of:

3 operating said ISP node to decapsulate said outer
4 connection; and

5 operating said client node to decapsulate said inner
6 connection.

1 14. The method of claim 13, further comprising the step of:

2 tunneling packets across said communication network
3 using Layer 2 Tunnel Protocol (L2TP).

1 15. System for nesting connections between a plurality of
2 nodes in a communication network, comprising:

3 a first node on an outer connection for receiving a
4 request from a second node to establish a coincident
5 endpoint for nesting an inner connection within said
6 outer connection;

7 said first and second nodes negotiating over said outer
8 connection parameters defining said inner connection;
9 and thereafter

10 said first node being responsive to communication
11 occurring on said inner connection for linking to said
12 outer connection for selectively receiving or sending
13 said communication double nested on said outer
14 connection.

1 16. The system of claim 15, said inner connection being a
2 secure connection.

1 17. The system of claim 16, said inner connection being an
2 IPsec connection.

1 18. The system of claim 17, further comprising a Layer 2
2 Tunnel Protocol (L2TP) connection for tunneling packets
3 across said communication network.

1 19. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable
3 by a machine to perform method steps for nesting
4 connections between a plurality of nodes in a

5 communication network, said method steps comprising:

6 receiving at a first node on an outer connection a
7 request from a second node to establish a coincident
8 endpoint for nesting an inner connection within said
9 outer connection;

10 negotiating over said outer connection parameters
11 defining said inner connection; and thereafter

12 responsive to communication occurring on said inner
13 connection, at said first node linking to said outer
14 connection for selectively receiving or sending said
15 communication double nested on said outer connection.

1 20. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable
3 by a machine to perform method steps for operating an
4 enterprise gateway, said method steps comprising:

5 receiving at said gateway from a remote client a
6 request to establish an outer connection;

7 receiving at said gateway over said outer connection a
8 request to establish, and thereupon negotiating
9 parameters establishing, a secure inner connection;

10 responsive to outbound or inbound traffic on said inner
11 connection, establishing links to said outer connection
12 for communicating said traffic double nested on said
13 outer connection.

1 21. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable
3 by a machine to perform method steps for operating a
4 first one of a plurality of nodes in a communications
5 network, comprising the steps of:

6 establishing at said first node a coincident endpoint
7 for an outer connection and an inner connection with at
8 least one second node in said network;

9 responsive to starting communication of traffic over
10 said connections, establishing a link from said inner
11 connection to said outer connection; and

12 responsive to said links, selectively encapsulating

13 said traffic to said outer connection for transfer to
14 said second node or decapsulating said traffic from
15 said outer connection for receipt at said first node.

1 22. A computer program product or computer program element
2 for nesting connections between a plurality of nodes in
3 a communication network according to steps comprising:

4 receiving at a first node on an outer connection a
5 request from a second node to establish a coincident
6 endpoint for nesting an inner connection within said
7 outer connection;

8 negotiating over said outer connection parameters
9 defining said inner connection; and thereafter

10 responsive to communication occurring on said inner
11 connection, at said first node linking to said outer
12 connection for selectively receiving or sending said
13 communication double nested on said outer connection.

1 23. A computer program product or computer program element
2 for perform method steps for operating an enterprise
3 gateway according to method steps comprising:

4 receiving at said gateway from a remote client a
5 request to establish an outer connection;

6 receiving at said gateway over said outer connection a
7 request to establish, and thereupon negotiating
8 parameters establishing, a secure inner connection;

9 responsive to outbound or inbound traffic on said inner
10 connection, establishing links to said outer connection
11 for communicating said traffic double nested on said
12 outer connection.

1 24. A computer program product or computer program element
2 for operating a first one of a plurality of nodes in a
3 communications network according to method steps
4 comprising:

5 establishing at said first node a coincident endpoint
6 for an outer connection and an inner connection with at
7 least one second node in said network;

